UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION

This Document Relates To:

GREGORY BLOCH, MADISON BRUECK, HOLLY BURKE, BEN DIECK, VICTOR DILUIGI, S.K. and M.K. (minors through their legal guardian), SHELLIE HARPER MCCASKELL, ELAINE MCCOY, TOMMY NICOLAS, ROBERT PLOTKE, JVANNE RHODES, M.P., K.S., and M.Y.(minors through their legal guardian), and RANIKA SMITH, on behalf of themselves and others similarly situated,

Plaintiffs,

v.

PROGRESS SOFTWARE CORPORATION and MAXIMUS FEDERAL SERVICES, INC.,

Defendants.

MDL No. 1:23-md-03083-ADB-PGL

DIRECT FILED COMPLAINT & JURY DEMAND PURSUANT TO MDL ORDER NO. 12

Civil Action No.

Plaintiffs Gregory Bloch, Madison Brueck, Holly Burke, Ben Dieck, Victor Diluigi, S.K. and M.K. (minors through their legal guardian), Shellie Harper McCaskell, Elaine McCoy, Tommy Nicolas, Robert Plotke, Jvanne Rhodes, M.P., K.S., and M.Y. (minors through their legal guardian), and Ranika Smith (collectively, "Plaintiffs") individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves and on information and belief as to all other matters, bring this Class Action Complaint against Defendants Progress Software

Corporation ("PSC") and Maximus Federal Services, Inc. ("Maximus") (collectively with PSC, "Defendants"), and in support thereof allege as follows:

NATURE OF ACTION

1. This Complaint is being directly filed into this MDL proceeding pursuant to the Court's MDL Order No. 12.

2. Plaintiffs incorporate the allegations contained in the Common Statement of Facts (ECF No. 908) in its entirety.

3. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard Plaintiffs' and other similarly situated patients' Personally Identifiable Information ("PII") and Protected Health Information ("PHI") (collectively, "Private Information" or "PI").

4. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[1] PHI is deemed private under the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq.*, as well as multiple state statutes. According to the U.S. Department of Health & Human Services ("HHS"), PHI "is information, including demographic data," that relates to: "the individual's past, present or future physical or mental health or condition," "the provision of health care to the individual," or "the past, present, or future payment for the provision of health care to the individual," and that "identifies the individual or for which there is a reasonable basis to believe

[1] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED*) at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.

it can be used to identify the individual." Individually identifiable health information includes many common identifiers (*e.g.*, name, address, birth date, SSN)."[2]

5. As used throughout this Complaint and previously defined in paragraph 3, "Private Information" is further defined as all information exposed by the Data Breach, including all or any part or combination of name, address, birth date, SSN, PHI, driver's license information (including license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or dispute documents with PII (such as images of government-issued identifications).

PARTIES

6. Plaintiff Gregory Bloch is, and was at all relevant times, an individual and citizen of Fleming Island, Florida.

7. Plaintiff Madison Brueck is, and was at all relevant times, an individual and citizen of Quincy, Illinois.

8. Plaintiff Holly Burke is, and was at all relevant times, an individual and citizen of Porter, Texas.

9. Plaintiff Ben Dieck is, and was at all relevant times, an individual and citizen of Fayetteville, North Carolina.

10. Plaintiff Victor Diluigi is, and was at all relevant times, an individual and citizen of York, Pennsylvania.

11. Plaintiffs S.K. and M.K., minors, are and at all relevant times were, individuals and residents of Sanford, Florida. S.K. and M.K. bring this suit by and through their father and legal

[2] *See Summary of the HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited June 5, 2024).

guardian, Aunali Khaku, who is, and was at all relevant times, an individual and citizen of Sanford, Florida.

12. Plaintiff Shellie Harper McCaskell is, and was at all relevant times, an individual and citizen of Hemet, California.

13. Plaintiff Elaine McCoy is, and was at all relevant times, an individual and citizen of Tiffin, Ohio.

14. Plaintiff Tommy Nicolas is, and was at all relevant times, an individual and citizen of Hempstead, New York.

15. Plaintiff Robert Plotke is, and was at all relevant times, an individual and citizen of Plainfield, Illinois.

16. Plaintiff Jvanne Rhodes is, and was at all relevant times, an individual and citizen of Dallas, Texas

17. Plaintiffs M.P., K.S., and M.Y., minors, are and at all relevant times were, individuals and residents of Allen, Texas. M.P., K.S., and M.Y. bring this suit by and through their mother and legal guardian, Aldreamer Smith, who is, and was at all relevant times, an individual and citizen of Allen, Texas.

18. Plaintiff Ranika Smith is, and was at all relevant times, an individual and citizen of Augusta, Georgia.

19. PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the data breach ("Data Breach") underlying Plaintiffs' claims.

20. Defendant Maximus Federal Services, Inc. is a Virginia corporation and maintains its headquarters and principal place of business at 1600 Tysons Boulevard, McLean, Virginia 22102.

JURISDICTION

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000) and is a class action in which one or more Class Members are citizens of states different from Defendants.

22. Absent the Court's MDL Order No. 12 (Direct Filing Order), Plaintiffs would have otherwise filed the case in each district court noted below, with the following bases:

a. Plaintiff Gregory Bloch would have filed his action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Bloch's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Bloch's claims occurred in that district.

b. Plaintiff Madison Brueck would have filed her action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that

district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Brueck's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Brueck's claims occurred in that district.

c. Plaintiff Holly Burke would have filed her action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Burke's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Burke's claims occurred in that district.

d. Plaintiff Ben Dieck would have filed his action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Dieck's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia

pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Dieck's claims occurred in that district.

e. Plaintiff Victor Diluigi would have filed his action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Diluigi's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Diluigi's claims occurred in that district.

f. Plaintiffs S.K. and M.K. would have filed this action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiffs S.K. and M.K.'s claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs S.K. and M.K.'s claims occurred in that district.

g. Plaintiff Shellie Harper McCaskell would have filed her action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is

located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff McCaskell's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff McCaskell's claims occurred in that district.

h. Plaintiff Elaine McCoy would have filed her action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff McCoy's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff McCoy's claims occurred in that district.

i. Plaintiff Tommy Nicolas would have filed his action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Nicolas's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia

pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Nicolas's claims occurred in that district.

j. Plaintiff Robert Plotke would have filed his action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Plotke's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Plotke's claims occurred in that district.

k. Plaintiff Jvanne Rhodes would have filed her action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Rhodes's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Rhodes's claims occurred in that district.

l. Plaintiffs M.P., K.S., and M.Y. would have filed this action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is

located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiffs M.P., K.S., and M.Y.'s claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiffs M.P., K.S., and M.Y..'s claims occurred in that district.

m. Plaintiff Ranika Smith would have filed her action in the United States District Court for the Eastern District of Virginia, Alexandria Division. That court has general jurisdiction over Defendant Maximus because Maximus's corporate headquarters is located in that district. That court has specific jurisdiction over Defendant PSC because PSC purposefully availed itself of the privilege of conducting business with Maximus in that district and Plaintiff Smith's claims arise from that business such that the exercise of jurisdiction would not offend traditional notions of fair play or substantial justice. Venue would be proper in the Eastern District of Virginia pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to Plaintiff Smith's claims occurred in that district.

FACTUAL ALLEGATIONS

Nature of Maximus's Business

23. Maximus primarily contracts with government agencies to provide services to manage and administer government-sponsored programs, including Medicare and Medicaid. Maximus provides medical evaluations, review of eligibility appeals, enrollment assistance, data analysis, and IT and consulting services.[3] Regarding Medicare specifically, Defendant reviews

[3] *Our Company*, Maximus, https://maximus.com/our-company (last accessed June 10, 2024).

"more than 600,000 appeals claims a year for Medicare" patients who experienced "health insurance denials."[4]

24. Maximus is the largest provider of government-sponsored benefit appeals programs in the United States. Defendant currently employs approximately 39,000 individuals and generates more than four billion dollars in annual revenue.[5]

25. As a condition of performing its services, Maximus requires that its government and corporate customers entrust it with highly sensitive Private Information belonging to Plaintiffs and Class Members.

26. Maximus' website promises consumers that Maximus has robust systems and processes in place to protect and secure their sensitive information.

> Securing every aspect of your mission: We are relentless in our pursuit to protect critical data, operations, and infrastructures. We go beyond traditional security measures to harden enterprise defenses for continuous mission protection.[6]

27. Maximus's website assures consumers—such as Plaintiffs and Class Members—that Maximus is an "expert" in cybersecurity:

> At Maximus, we are relentless in our pursuit of protecting enterprise assets, data, and operations Trusted to manage some of the government's largest security operations, we leverage our deep knowledge of agency mission and extensive technical expertise to create integrated cyber solutions that bolster enterprise cyber defenses for continual mission protection.[7]

---

[4] *Centers for Medicare and Medicaid*, Maximus, https://maximus.com/cms (last accessed June 10, 2024).
[5] *Our Company*, Maximus https://maximus.com/our-company (last accessed June 10, 2024).
[6] *Cybersecurity*, Maximus https://maximus.com/cybersecurity (last accessed June 10, 2024).
[7] *Maximus Cybersecurity Capabilities*, Maximus (2023), *available at* https://maximus.com/sites/default/files/documents/Federal/Maximus_Cybersecurity-Capabilities-Overview.pdf (last accessed June 10, 2024).

28. Maximus's website repeatedly states that it is keenly cognizant of data privacy risks and has adequate procedures and process in place to prevent them, including its statements that:

- "We strengthen cyber resiliency, protecting critical data, operations, and infrastructures for continual operational excellence. Our full-spectrum cybersecurity services offer unrivaled cyber defense against the most advanced cyber adversaries. From zero trust to secure application development, we deliver next-gen cyber technologies and solutions that address today's most complex security challenges."[8]
- "To defend against today's sophisticated cyber adversaries, Maximus goes beyond traditional security measures to harden enterprise security and continuously protect the mission."[9]
- "Maximus uses various technological and procedural security measures in order to protect the personal information we collect through the Site from loss, misuse, alteration or destruction. We have documented Information Security & Privacy policies to address data protection. We regularly provide information security and privacy awareness training to our employees."[10]
- "We have prepared a formal incident response plan in case of a data breach."[11]
- "All employees, including full-time and part-time permanent and temporary employees, complete mandatory data privacy and security training on an annual

[8] *Technology Consulting Services*, Maximus https://maximus.com/technology-consulting-services (last accessed June 10, 2024).
[9] *Cybersecurity*, Maximus, https://maximus.com/cybersecurity (last accessed June 10, 2024).
[10] *Our Commitment to Privacy*, Maximus, https://maximus.com/privacy-statement (last accessed June10, 2024).
[11] *Id*.

basis .... We supplement the annual training with ongoing training in multiple mediums. Training topics include, but are not limited, to the following: • Data protection principles regarding the use, protection, storage, transmission, and disposal of confidential information, with a specific focus on how certain data may not be used." [12]

- "Maximus developed a robust incident management process to respond to a wide variety of cyber incidents globally. This process includes triage, investigation, evidence collection and storage, root cause analysis, and incident resolution with executive reporting."[13]

29. Maximus also touts its data security accreditations, including an ISO/IEC 20000-1 certification, and NCQA Accreditation.[14]

30. Yet, contrary to Maximus's website representations—by virtue of Maximus's admissions that it experienced the Data Breach which revealed the Private Information of more than 11 million individuals—Maximus did not have adequate measures in place to protect and maintain sensitive Private Information entrusted to it or to ensure its vendors and business associates reasonably or adequately secured, safeguarded, and otherwise protected consumers' Private Information that Maximus shared with third-party vendors such as PSC through Maximus's use of MOVEit. Instead, Maximus's website wholly fails to disclose the truth: that Maximus lacks sufficient processes to protect the Private Information that is entrusted to it.

Maximus and PSC Failed to Protect Plaintiffs' and Class Members' Private Information

[12] *Building a Better Future Together 2023 Sustainability Report*, Maximus, https://sprcdn-assets.sprinklr.com/3774/c8c4202f-e7cb-4d98-aa47-825dc7f8cdbb-2399725906.pdf (last accessed June 10, 2024).
[13] *Id*.
[14] *Our Company*, Maximus https://maximus.com/our-company (last accessed June 10, 2024).

31. Defendants had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of their IT vendors' and affiliates' data security practices and systems. Defendants had a legal duty to keep Private Information safe and confidential.

32. Defendants had obligations created by the FTC Act, HIPAA, contract, industry standards, representations made to Plaintiffs and Class Members, and common law to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

33. Defendants derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendants could not perform the services they provide.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

Plaintiffs' Experiences with the Data Breach

Plaintiff Bloch

35. In approximately 2008, Plaintiff Gregory Bloch's (now adult) children received medical services through Florida Healthy Kids Corporation.

36. In order for his children to obtain medical services through Medicaid, Plaintiff Bloch was required to provide his Private Information to Maximus, directly or indirectly, including his name, Social Security number, date of birth, contact information, and other sensitive information.

37. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Bloch's Private Information in its system and shared it with its IT vendors.

38. Plaintiff Bloch is very careful about sharing his sensitive Private Information. He stores any documents containing his Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Bloch would not have entrusted his Private Information to Maximus had he known of Maximus's lax data security policies.

39. Plaintiff Bloch received a Notice Letter dated August 25, 2023, by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Bloch's Private Information – including name, address, date of birth, Social Security number, email address, phone number, and "other governmental issued identifier" – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Bloch has suffered a loss of value of his Private Information.

40. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Bloch has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting card issuers and/or banks to preemptively get new numbers issued, monitoring accounts for suspicious activity, investigating suspicious activity, contacting banks, credit card companies, and/or other businesses about suspicious activity, and filing a complaint with the FTC. Plaintiff Bloch has spent significant time dealing with the Data Breach—valuable time Plaintiff Bloch otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Bloch

estimates that he has spent approximately 22 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

41. Plaintiff Bloch has also experienced actual fraudulent activities as a result of the Data Breach. Plaintiff Bloch has incurred fraudulent charges on his debit card, which caused him to cancel his debit card in or about June 2023. Plaintiff Bloch has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

42. The Data Breach has caused Plaintiff Bloch to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed him of key details about the Data Breach's occurrence.

43. As a result of the Data Breach, Plaintiff Bloch anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Bloch is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Brueck

44. Plaintiff Madison Brueck has no known relationship with Colorado Department of Human Services or Maximus. Yet at the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Brueck's Private Information in its system and shared it with its IT vendors.

45. Plaintiff Brueck is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Brueck would not have entrusted her Private Information to Maximus had she known of Maximus's lax data security policies.

46. Plaintiff Brueck received a Notice Letter dated August 24, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Brueck's Private Information – including name, address, date of birth, and Social Security number – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Brueck has suffered a loss of value of her Private Information.

47. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Brueck has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, checking her report for suspicious activity, and contacting her credit card company to turn on notifications on for purchases over $50. Plaintiff Brueck has spent significant time dealing with the Data Breach–valuable time Plaintiff Brueck otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Brueck estimates that she has spent approximately 7 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

48. Plaintiff Brueck has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, Plaintiff Brueck has experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

49. The Data Breach has caused Plaintiff Brueck to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed her of key details about the Data Breach's occurrence.

50. As a result of the Data Breach, Plaintiff Brueck anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data

Breach. Plaintiff Brueck is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Burke

51. Plaintiff Holly Burke has received Medicaid services through Texas Health and Human Services.

52. In order to obtain medical services through Medicaid, Plaintiff Burke was required to provide her Private Information to Maximus, directly or indirectly, including her name, Social Security number, date of birth, contact information, and other sensitive information.

53. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Burke's Private Information in its system and shared it with its IT vendors.

54. Plaintiff Burke is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Burke would not have entrusted her Private Information to Maximus had she known of Maximus's lax data security policies.

55. Plaintiff Burke received the Notice Letter dated August 31, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Burke's Private Information – including name, address, date of birth, Social Security number, email address, telephone number, and treatment dates – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Burke has suffered a loss of value of her Private Information.

56. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Burke has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting major credit bureaus to freeze her credit, contacting card issuers and/or banks to preemptively get new numbers issued, monitoring accounts for suspicious activity, investigating suspicious activity, contacting banks, credit card companies, and/or other businesses about suspicious activity, and filing a complaint with the FTC. Plaintiff Burke has spent significant time dealing with the Data Breach—valuable time Plaintiff Burke otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Burke estimates that she has spent approximately 200 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

57. Plaintiff Burke has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, someone accessed her Medicaid benefits account and changed her information. In addition, Plaintiff Burke has experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

58. The Data Breach has caused Plaintiff Burke to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed him of key details about the Data Breach's occurrence.

59. As a result of the Data Breach, Plaintiff Burke anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Burke is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Dieck

60. Plaintiff Benjamin Dieck has no known relationship with Colorado Department of Human Services or Maximus. Yet at the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Dieck's Private Information in its system and shared it with its IT vendors.

61. Plaintiff Dieck is very careful about sharing his sensitive Private Information. He stores any documents containing his Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Dieck would not have entrusted his Private Information to Maximus had he known of Maximus's lax data security policies.

62. Plaintiff Dieck received a Notice Letter dated August 24, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Dieck's Private Information – including name, address, date of birth, and Social Security number – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Dieck has suffered a loss of value of his Private Information.

63. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Dieck has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach and monitoring his accounts for suspicious activity. Plaintiff Dieck has spent significant time dealing with the Data Breach—valuable time Plaintiff Dieck otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Dieck estimates that he has spent approximately 25 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

64. Plaintiff Dieck has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, Plaintiff Dieck has experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

65. The Data Breach has caused Plaintiff Dieck to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed him of key details about the Data Breach's occurrence.

66. As a result of the Data Breach, Plaintiff Dieck anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Dieck is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Diluigi

67. Plaintiff Victor Diluigi has no known relationship with the Arkansas Division of Workforce Services or Maximus. Yet at the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Diluigi's Private Information in its system and shared it with its IT vendors.

68. Plaintiff Diluigi is very careful about sharing his sensitive Private Information. He stores any documents containing his Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Diluigi would not have entrusted his Private Information to Maximus had he known of Maximus's lax data security policies.

69. Plaintiff Diluigi received a Notice Letter dated September 29, 2023 by U.S. mail, from Maximus. According to the Notice Letter, Plaintiff Diluigi's Private Information – including name, address, date of birth, and Social Security number – may have been improperly accessed

and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Diluigi has suffered a loss of value of his Private Information.

70. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Diluigi has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting Maximus and/or Arkansas Division of Workforce Services about the Data Breach, contacting card issuers/banks to preemptively get new numbers, major credit bureaus to freeze her credit, contacting card issuers and/or banks to preemptively get new numbers issues, monitoring accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and/or other businesses about suspicious activity. Plaintiff Diluigi has spent significant time dealing with the Data Breach—valuable time Plaintiff Diluigi otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Diluigi estimates that he has spent approximately 48 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

71. Plaintiff Diluigi has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, Plaintiff Diluigi has experienced multiple unauthorized charges on his credit card and his debit card as well as a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

72. Plaintiff Diluigi has also incurred out-of-pocket expenses as a result of the Data Breach. More specifically, Plaintiff has unreimbursed fraudulent credit card charges and monthly identity theft insurance payments.

73. The Data Breach has caused Plaintiff Diluigi to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed him of key details about the Data Breach's occurrence.

74. As a result of the Data Breach, Plaintiff Diluigi anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Diluigi is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiffs S.K. and M.K.

75. Plaintiffs S.K. and M.K. have received medical services through Florida Healthy Kids Corporation.

76. In order to have their medical claims processed, Plaintiffs S.K. and M.K.'s father and legal guardian, Aunali Khaku, was required to provide his children's Private Information to Maximus, directly or indirectly, including their name, Social Security numbers, dates of birth, contact information, and other sensitive information.

77. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiffs S.K. and M.K.'s Private Information in its system and shared it with its IT vendors.

78. Plaintiffs S.K. and M.K.'s father, Aunali Khaku, is very careful about sharing his family's sensitive Private Information. He stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Aunali Khaku would not have entrusted his family's, including Plaintiffs S.K. and M.K.'s, Private Information to Maximus had he known of Maximus's lax data security policies.

79. Plaintiffs S.K. and M.K. received Notice Letters dated August 11, 2023 by U.S. mail, directly from Maximus. According to the Notice Letters, Plaintiffs S.K. and M.K.'s Private Information – including name, address, date of birth, and Social Security number– may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiffs S.K. and M.K. have suffered a loss of value of their Private Information.

80. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiffs S.K. and M.K., through their father Aunali Khaku, have made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting Maximus about the Data Breach, monitoring accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and/or other businesses about suspicious activity. Plaintiffs S.K. and M.K., through their father Aunali Khaku, have spent significant time dealing with the Data Breach—valuable time that otherwise would have been spent on other activities, including but not limited to work and/or recreation. All told, Plaintiffs S.K. and M.K., through their father Aunali Khaku, estimate that they have spent approximately 20 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

81. Plaintiffs S.K. and M.K., through their father Aunali Khaku, have also experienced actual fraudulent activities as a result of the Data Breach, such as a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

82. The Data Breach has caused Plaintiffs S.K. and M.K., through their father Aunali Khaku, to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed them of key details about the Data Breach's occurrence.

83. As a result of the Data Breach, Plaintiffs S.K. and M.K., through their father Aunali Khaku, anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiffs S.K. and M.K. are presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff McCaskell

84. Plaintiff Shellie Harper McCaskell has received healthcare services from Medicare through the Centers for Medicare & Medicaid Services.

85. In order to obtain medical services through Medicare, Plaintiff McCaskell was required to provide her Private Information to Maximus, directly or indirectly, including her name, Social Security number, date of birth, contact information, and other sensitive information.

86. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff McCaskell's Private Information in its system and shared it with its IT vendors.

87. Plaintiff McCaskell is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff McCaskell would not have entrusted her Private Information to Maximus had she known of Maximus's lax data security policies.

88. Plaintiff McCaskell received a Notice Letter dated July 28, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff McCaskell's Private Information – including name, address, date of birth, Social Security number, email address, telephone number, and medical history – may have been improperly accessed and obtained by unauthorized third

parties. As a result of the Data Breach, Plaintiff McCaskell has suffered a loss of value of her Private Information.

89. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff McCaskell has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, and reviewing her credit reports for suspicious activity. Plaintiff McCaskell has spent significant time dealing with the Data Breach–valuable time Plaintiff McCaskell otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff McCaskell estimates that she has spent approximately 8 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

90. Plaintiff McCaskell has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, Plaintiff McCaskell has experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

91. Plaintiff McCaskell has also incurred out-of-pocket expenses as a result of the Data Breach.

92. The Data Breach has caused Plaintiff McCaskell to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed her of key details about the Data Breach's occurrence.

93. As a result of the Data Breach, Plaintiff McCaskell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff McCaskell is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff McCoy

94. Plaintiff Elaine McCoy has received healthcare services from Medicare through the Centers for Medicare & Medicaid Services.

95. In order to obtain medical services through Medicare, Plaintiff McCoy was required to provide her Private Information to Maximus, directly or indirectly, including her name, Social Security number, date of birth, contact information, and other sensitive information.

96. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff McCoy's Private Information in its system and shared it with its IT vendors.

97. Plaintiff McCoy is very careful about sharing her sensitive Private Information. She stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff McCoy would not have entrusted her Private Information to Maximus had she known of Maximus's lax data security policies.

98. Plaintiff McCoy received a Notice Letter dated July 28, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff McCoy's Private Information – including name, address, date of birth, Social Security number, email address, telephone number, and medical history – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff McCoy has suffered a loss of value of her Private Information.

99. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff McCoy has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for

suspicious activity, and contacting banks, credit card companies, and other businesses about suspicious activity. Plaintiff McCoy has spent significant time dealing with the Data Breach—valuable time Plaintiff McCoy otherwise would have spent on other activities. All told, Plaintiff McCoy estimates that she has spent approximately 40 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

100. Plaintiff McCoy has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, Plaintiff McCoy has experienced unauthorized charges on multiple credit cards. Plaintiff McCoy successfully disputed the charges and then cancelled both credit cards. Plaintiff McCoy has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

101. The Data Breach has caused Plaintiff McCoy to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed her of key details about the Data Breach's occurrence.

102. As a result of the Data Breach, Plaintiff McCoy anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff McCoy is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Nicolas

103. Plaintiff Tommy Nicolas has no known relationship with the Colorado Department of Human Services, Division of Child Support Services or Maximus. Yet at the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Nicolas's Private Information in its system and shared it with its IT vendors.

104. Plaintiff Nicolas is very careful about sharing his sensitive Private Information. He stores any documents containing his Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Nicolas would not have entrusted his Private Information to Maximus had he known of Maximus's lax data security policies.

105. Plaintiff Nicolas received a Notice Letter dated August 24, 2023 by U.S. mail, from Maximus. According to the Notice Letter, Plaintiff Nicolas's Private Information – including name, address, date of birth, and Social Security number – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Nicolas has suffered a loss of value of his Private Information.

106. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Nicolas has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach and monitoring accounts for suspicious activity. Plaintiff Nicolas has spent significant time dealing with the Data Breach—valuable time Plaintiff Nicolas otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Nicolas estimates that he has spent approximately 75 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

107. Plaintiff Nicolas has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, Plaintiff Nicolas has experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

108. The Data Breach has caused Plaintiff Nicolas to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed him of key details about the Data Breach's occurrence.

109. As a result of the Data Breach, Plaintiff Nicolas anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Nicolas is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Plotke

110. Plaintiff Robert Plotke has received healthcare services from Medicare and has been covered by certain Financial Institution Data Matching laws.

111. In order to obtain medical services through Medicare, Plaintiff Plotke was required to provide his Private Information to Maximus, directly or indirectly, including his name, Social Security number, date of birth, contact information, and other sensitive information. Also, because Plaintiff Plotke was covered by certain Financial Institution Data Matching laws, Maximus obtained, directly or indirectly, Plaintiff Plotke's Private Information, including his name, Social Security number, date of birth, contact information, and other sensitive information.

112. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Plotke's Private Information in its system and shared it with its IT vendors.

113. Plaintiff Plotke is very careful about sharing his sensitive Private Information. He stores any documents containing her Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any

other unsecured source. Plaintiff Plotke would not have entrusted his Private Information to Maximus had he known of Maximus's lax data security policies.

114. Plaintiff Plotke received a Notice Letter dated November 30, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Plotke's Private Information – including name, address, date of birth, Social Security number, and financial account number – may have been improperly accessed and obtained by unauthorized third parties. According to the Notice Letter, Plaintiff Plotke's information was shared with Maximus by financial institutions that do business in Minnesota in accordance with Financial Institution Data Matching laws. As a result of the Data Breach, Plaintiff Plotke has suffered a loss of value of his Private Information.

115. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Plotke has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring his accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and other businesses about suspicious activity. Plaintiff Plotke has spent significant time dealing with the Data Breach–valuable time Plaintiff Plotke otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Plotke estimates that he has spent approximately 45 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

116. Plaintiff Plotke has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, a credit card was opened in Plaintiff Plotke's name without his permission. Plaintiff Plotke has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

117. Plaintiff Plotke has also incurred out-of-pocket expenses as a result of the Data Breach.

118. The Data Breach has caused Plaintiff Plotke to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed him of key details about the Data Breach's occurrence.

119. As a result of the Data Breach, Plaintiff Plotke anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Plotke is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Rhodes

120. Plaintiff Jvanne Rhodes's four children are enrolled with and received healthcare services from the Texas Health and Human Services Commission.

121. In order for her children to obtain medical services, Plaintiff Rhodes was required to provide her Private Information to Maximus, directly or indirectly, including her name, Social Security number, date of birth, contact information, and other sensitive information.

122. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Rhodes's Private Information in its system and shared it with its IT vendors.

123. Plaintiff Rhodes is very careful about sharing her sensitive Private Information. She stores any documents containing his Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Rhodes would not have entrusted her Private Information to Maximus had she known of Maximus's lax data security policies.

124. Plaintiff Rhodes received a Notice Letter dated August 31, 2023, by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Rhodes' Private Information – including name, address, date of birth, Social Security number, email address, phone number, and dates of service– may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Rhodes has suffered a loss of value of her Private Information.

125. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Rhodes has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting Maximus and/or the Texas Health and Human Services Commission about the Data Breach, contacting credit bureaus to freeze her credit, monitoring accounts for suspicious activity, investigating suspicious activity, contacting banks, credit card companies, and/or other businesses about suspicious activity, and filing a police report regarding unauthorized charges on her debit cards. Plaintiff Rhodes has spent significant time dealing with the Data Breach—valuable time Plaintiff Rhodes otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Rhodes estimates that she has spent approximately 85 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

126. Plaintiff Rhodes has also experienced actual fraudulent activities as a result of the Data Breach. Plaintiff Rhodes has incurred multiple fraudulent charges on two debit cards, which caused her to cancel both of them. However, Plaintiff Rhodes continues to experience recurring fraudulent charges. Plaintiff Rhodes has also been notified that an unknown person has tried to open accounts in her name without her authorization. Also, an unknown person in Houston has

attempted to obtain unemployment benefits in Plaintiff Rhodes's name. Plaintiff Rhodes has also experienced a large uptick in fraudulent spam and phishing calls and emails since the Data Breach.

127. Plaintiff Rhodes has also incurred out-of-pocket expenses as a result of the Data Breach. More specifically, Plaintiff Rhodes has incurred overdraft/late fees caused by fraudulent charges on her accounts. And although Plaintiff Rhodes has been reimbursed by her bank for some of the unauthorized charges she has experienced, there are some charges that are still under investigation.

128. The Data Breach has caused Plaintiff Rhodes to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed her of key details about the Data Breach's occurrence.

129. As a result of the Data Breach, Plaintiff Rhodes anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Rhodes is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiffs M.P., K.S., and M.Y.

130. Plaintiffs M.P., K.S., and M.Y. have received healthcare services from the Texas Health and Human Services Commission.

131. In order to receive medical services, Plaintiffs M.P., K.S., and M.Y.'s mother and legal guardian, Aldreamer Smith, was required to provide her children's Private Information to Maximus, directly or indirectly, including their names, Social Security numbers, dates of birth, contact information, and other sensitive information.

132. At the time of the Data Breach – approximately May 27, 2023, through May 31, 2023 – Maximus retained Plaintiffs M.P., K.S., and M.Y.'s Private Information in its system and shared it with its IT Vendors.

133. Plaintiffs M.P., K.S., and M.Y.'s mother, Aldreamer Smith, is very careful about sharing her family's sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Aldreamer Smith would not have entrusted her family's, including M.P., K.S., and M.Y.'s, Private Information to Maximus had she known of Maximus's lax data security policies.

134. Plaintiffs M.P. and M.Y. received Notice Letters dated September 9, 2023 by U.S. mail, directly from Maximus. Plaintiff K.S. received a Notice Letter dated August 31, 2023 by U.S. mail, directly from Maximus. According to the Notice Letters, Plaintiffs M.P., K.S., and M.Y.'s Private Information – including names, dates, of birth, and Social Security numbers – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiffs M.P., K.S., and M.Y. have suffered a loss of value of their Private Information.

135. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiffs M.P., K.S., and M.Y., through their mother Aldreamer Smith, have made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, contacting credit bureaus, monitoring accounts for suspicious activity, investigating suspicious activity, and contacting banks, credit card companies, and/or other businesses about suspicious activity. Plaintiffs M.P., K.S., and M.Y., through their mother Aldreamer Smith, have spent significant time dealing with the Data Breach—valuable time that otherwise would have spent on other activities, including but not limited to work and/or recreation.

All told, Plaintiffs M.P., K.S., and M.Y., through their mother Aldreamer Smith, estimate that they have spent approximately 8 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

136. Plaintiffs M.P., K.S., and M.Y., through their mother Aldreamer Smith, have also experienced actual fraudulent activities as a result of the Data Breach. More specifically, an unknown third party attempted to make unauthorized charges on K.S.'s bank card, which caused the account to be closed. Moreover, M.P., K.S., and M.Y., through their mother Aldreamer Smith, have experienced a large uptick in fraudulent solicitations and spam mail, such as for credit cards and internet services, since the Data Breach.

137. The Data Breach has caused Plaintiffs M.P., K.S., and M.Y., through their mother Aldreamer Smith, to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed them of key details about the Data Breach's occurrence.

138. As a result of the Data Breach, Plaintiffs M.P., K.S., and M.Y., through their mother Aldreamer Smith, anticipate spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. M.P., K.S., and M.Y. are presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Smith

139. Plaintiff Ranika Smith has received Medicaid services through the Georgia Department of Community Health.

140. In order to obtain Medicaid services, Plaintiff Smith was required to provide her Private Information to Maximus, directly or indirectly, including their name, Social Security numbers, dates of birth, contact information, and other sensitive information.

141. At the time of the Data Breach—approximately May 27, 2023, through May 31, 2023—Maximus retained Plaintiff Smith's Private Information in its system and shared it with its IT vendors.

142. Plaintiff Smith is very careful about sharing her sensitive Private Information. She stores any documents containing Private Information in a safe and secure location and has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Smith would not have entrusted her Private Information to Maximus had she known of Maximus's lax data security policies.

143. Plaintiff Smith received a Notice Letter dated October 10, 2023 by U.S. mail, directly from Maximus. According to the Notice Letter, Plaintiff Smith's Private Information – including name, address, date of birth, Social Security number, email address, phone number, and Client ID – may have been improperly accessed and obtained by unauthorized third parties. As a result of the Data Breach, Plaintiff Smith has suffered a loss of value of her Private Information.

144. As a result of the Data Breach, and at the direction of Maximus's Notice Letter, Plaintiff Smith has made reasonable efforts to mitigate the impact of the Data Breach, which has included researching and verifying the legitimacy of the Data Breach, monitoring her accounts for suspicious activity, investigating any suspicious activity she found, and contacting banks, credit card companies, and/or other businesses about the suspicious activity. Plaintiff Smith has spent significant time dealing with the Data Breach—valuable time Plaintiff Smith otherwise would have spent on other activities, including but not limited to work and/or recreation. All told, Plaintiff Smith estimates that she has spent approximately 45 hours to date responding to the Data Breach. This time has been lost forever and cannot be recaptured.

145. Plaintiff Smith has also experienced actual fraudulent activities as a result of the Data Breach. More specifically, unknown third parties have attempted to access Plaintiff Smith's accounts on multiple occasions and have attempted to open a new credit card account in Plaintiff Smith's name without her authorization. Someone also tried to take out a payday loan in Plaintiff Smith's name.

146. Plaintiff Smith has also incurred out-of-pocket expenses as a result of the Data Breach. More specifically, Plaintiff Rhodes enrolled in the LifeLock service at a cost of $279 per year as a result of the Data Breach.

147. The Data Breach has caused Plaintiff Smith to suffer fear, anxiety, and stress, which has been compounded by the fact that Maximus has still not fully informed her of key details about the Data Breach's occurrence.

148. As a result of the Data Breach, Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Smith is presently at risk and will continue to be at increased risk of identity theft and fraud for years to come.

CLASS ALLEGATIONS

149. Plaintiffs bring this action on behalf of themselves and on behalf of the following Class: "All residents of the United States whose PHI and/or PII was compromised as a result of the Data Breach" (the "Nationwide Class").

150. Plaintiffs also bring this action on behalf of themselves and on behalf of the following subclass: "All residents of the United States whose PHI and/or PII was maintained by Maximus when it was compromised as a result of the Data Breach" (the "Maximus Subclass").

151. Plaintiff McCaskell also brings this action on behalf of herself and the following California Subclasses:

"All residents of California whose PHI and/or PII was compromised as a result of the Data Breach" (the "California Subclass"); and

"All residents of California whose PHI and/or PII was maintained by Maximus when it was compromised as a result of the Data Breach" (the "California Maximus Subclass").

152. The foregoing classes are referred to herein, collectively, as the "Class." Excluded from the Class are: (1) the judges presiding over the action; (2) the Defendants, their subsidiaries, parent companies, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest, and their current or former officers and directors; (3) persons who properly opt out; and (4) the successors or assigns of any such excluded persons.

153. **Numerosity**: Class Members are so numerous that their individual joinder is impracticable, as the proposed Class includes tens of millions of members who are geographically dispersed.

154. **Typicality**: Plaintiffs' claims are typical of Class Members' claims. Plaintiffs and all Class Members were injured through Defendants' uniform misconduct, and Plaintiffs' claims are identical to the claims of the Class Members they seek to represent.

155. **Adequacy**: Plaintiffs' interests are aligned with the Class they seek to represent and Plaintiffs have retained counsel with significant experience prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiffs and their counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiffs and undersigned counsel.

156. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Members' claims. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, because of the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

157. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

a. Whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' Private Information;

c. Whether Defendants breached their duties to protect Plaintiffs' and Class Members' Private Information;

d. Whether Defendants violated the statutes alleged herein;

e. Whether Plaintiffs and all other Class Members are entitled to damages and the measure of such damages and relief.

158. Given that Defendants engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
NEGLIGENCE
Brought on Behalf of the Nationwide Class Against PSC and on Behalf of the Maximus Subclass Against Maximus

159. Plaintiffs reallege and incorporate by reference the preceding paragraphs as if fully set forth herein.

160. Defendants knowingly collected, acquired, stored, and/or maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting the Private Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

161. The duty included obligations to take reasonable steps to prevent disclosure of the Private Information, and to safeguard the information from theft. Defendants' duties included the responsibility to design, implement, and monitor data security systems, policies, and processes to protect against reasonably foreseeable data breaches such as this Data Breach.

162. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, policies, and procedures, and the personnel responsible for them, adequately protected the Private Information.

163. These duties owed by Defendants included the obligation to properly review, assess, and manage the cybersecurity risk posed by third-party vendors and service providers.

164. Defendants owed a duty of care to safeguard the Private Information due to the foreseeable risk of a data breach and the severe consequences that would result from their failure to so safeguard the Private Information.

165. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and those individuals who entrusted them with their Private Information, which is recognized by laws and regulations as well as common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

166. Under HIPAA, Defendants had a duty to use reasonable security measures to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA. *Id*.

167. Moreover, under HIPAA, Defendants had a duty to render the electronic Private information that they maintained as unusable, unreadable, or indecipherable to unauthorized individuals. Specifically, the HIPAA Security Rule requires "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." 45 C.F.R. § 164.304 (defining encryption).

168. Plaintiffs and Class Members are within the class of persons that the HIPAA was intended to protect. And the injuries that Defendants inflicted on Plaintiffs and Class Members are precisely the harms that HIPAA guards against. After all, the Federal Health and Human Services' Office for Civil Rights ("OCR") has pursued enforcement actions against businesses which—

because of their failure to employ reasonable data security measures—caused the very same injuries that Defendants inflicted upon Plaintiffs and Class Members.

169. Under § 17932 of the Health Information Technology for Economic and Clinical Health Act ("HITECH"), Defendants have a duty to promptly notify "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach" the respective covered entities and affected persons so that the entities and persons can take action to protect themselves. 42 U.S.C.A. § 17932(d)(1).

170. Moreover, § 17932(a) of HITECH states that, "[a] covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach."

171. And § 17932(b) of HITECH states that, "[a] business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach."

172. Under the Federal Trade Commission Act ("FTCA"), Defendants had a duty to employ reasonable security measures. Specifically, this statute prohibits "unfair . . . practices in or

affecting commerce," including (as interpreted and enforced by the FTC) the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. § 45.

173. Moreover, Plaintiffs and Class Members' injuries are precisely the type of injuries that the FTCA guards against. After all, the FTC has pursued numerous enforcement actions against businesses that—because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices—caused the very same injuries that Defendants inflicted upon Plaintiffs and Class Members.

174. Defendants' duty to use reasonable care in protecting Private Information arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect Private Information that they acquire, maintain, or store.

175. Defendants owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to their Private Information. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the fallout of the Data Breach.

176. Defendants owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from its inadequate security protocols. After all, Defendants actively sought and obtained the Private Information of Plaintiffs and Class Members.

177. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information. And but for

Defendants' negligence, Plaintiffs and Class Members would not have been injured. The specific negligent acts and omissions committed by Defendants include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to comply with—and thus violating—HIPAA and its regulations;

c. Failing to comply with—and thus violating—HITECH and its regulations;

d. Failing to comply with—and thus violating—FTCA and its regulations;

e. Failing to adequately monitor the security of their networks and systems;

f. Failing to have in place mitigation policies and procedures;

g. Allowing unauthorized access to Class Members' Private Information;

h. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

i. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

178. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information, as alleged and discussed above.

179. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiffs and Class Members.

180. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the data transfer and storage industry.

181. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

182. The imposition of a duty of care on Defendants to safeguard the Private Information they maintained is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiffs and Class Members as a result of the Data Breach.

183. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained damages including: (i) invasion of privacy; (ii) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (iii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iv) financial "out-of-pocket" costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) loss of time due to increased spam and targeted marketing emails; (vii) loss of value of their Private Information; (viii) future costs of identity theft monitoring; (ix) anxiety, annoyance and nuisance, and (x) the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs and Class Members' Private Information.

184. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

185. Defendants' negligent conduct is ongoing, in that they still hold the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

186. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CLAIM FOR RELIEF
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
Brought on Behalf of the Maximus Subclass Against Maximus

187. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 186 as if fully set forth herein.

188. Upon information and belief, Maximus entered into contracts with its government and corporate customers to provide administrative services that included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was entrusted to it.

189. Such contracts were made expressly for the benefit of Plaintiffs and the Class Members, as it was their Private Information that Maximus agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class were the direct and primary objective of the contracting parties and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

190. Maximus knew or should have known that if it were to breach these contracts, Plaintiffs and Class Members would be harmed.

191. Maximus breached its contracts by, among other things, failing to adequately secure Plaintiffs' and Class Members' Private Information, and, as a result, Plaintiffs and Class Members were harmed by Defendants' failure to secure their Private Information.

192. As a direct and proximate result of Defendant's breach, Plaintiffs and Class Members are at a current and ongoing substantial risk of fraud and identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat

of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) loss of value of their Private Information; (vii) future costs of identity theft monitoring; (viii) and the continued risk to their Private Information, which remains in Maximus's control, and which is subject to further breaches, so long as Maximus fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

THIRD CLAIM FOR RELIEF
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
On Behalf of the Nationwide Class Against PSC

193. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 192 as if fully set forth herein.

194. Upon information and belief, PSC entered into contracts with its government and/or corporate customers to provide secure file transfer services that included data security practices, procedures, designs, and protocols sufficient to safeguard the Private Information that was entrusted to it.

195. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that PSC agreed to receive, store, utilize, transfer, and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

196. PSC knew or should have known that if it were to breach these contracts with its customers, Plaintiffs and Class Members would be harmed.

197. PSC breached its contracts with customers by, among other things, failing to adequately secure Plaintiffs' and Class Members' Private Information, and, as a result, Plaintiffs and Class Members were harmed by PSC's failure to secure their Private Information.

198. As a direct and proximate result of Defendant's breach, Plaintiffs and Class Members are at a current and ongoing risk of identity theft, and Plaintiffs and Class Members sustained incidental and consequential damages including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) loss of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in PSC's control, and which is subject to further breaches, so long as PSC fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

199. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

200. Plaintiff and Class Members are also entitled to injunctive relief requiring PSC to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate ID protection and credit monitoring to all Class Members.

FOURTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
Brought on Behalf of the Nationwide Class Against PSC and on Behalf of the Maximus Subclass Against Maximus

201. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 200 as if fully set forth herein, and they bring this claim for relief in the alternative to Plaintiffs' contract-based claims for relief.

202. Plaintiffs and Class Members conferred a monetary benefit on Defendants by providing Defendants with their valuable Private Information.

203. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information, which cost savings increased the profitability of the services.

204. Upon information and belief, instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

205. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

206. Defendants acquired the monetary benefit and Private Information, through inequitable means in that Defendants failed to disclose their inadequate security practices previously alleged.

207. Had Plaintiffs and Class Members known that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants. Plaintiffs and Class Members have no adequate remedy at law.

208. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

209. Furthermore, as a direct and proximate result of Defendants' unreasonable and inadequate data security practices, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (i) financial "out-of-pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (iii) financial "out-of-pocket" costs incurred due to actual identity theft; (iv) loss of time incurred due to actual identity theft; (v) loss of time due to increased spam and targeted marketing emails; (vi) loss of value of their Private Information; (vii) future costs of identity theft monitoring; and (viii) the continued risk to their Private Information, which remains in Defendants' control, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

210. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

211. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate ID theft and credit monitoring to all Class Members.

212. Moreover, Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly

received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

FIFTH CLAIM FOR RELIEF
DECLARATORY AND INJUNCTIVE RELIEF
Brought on Behalf of the Nationwide Class Against PSC and on Behalf of the Maximus Subclass Against Maximus

213. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 212 as if fully set forth herein.

214. Plaintiffs pursue this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

215. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

216. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

217. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect Plaintiffs' and Class Members' Private Information.

218. Defendants still control the Private Information of Plaintiffs and the Class Members.

219. To Plaintiffs' knowledge, Defendants have made no announcement that they have changed their data or security practices relating to the Private Information.

220. To Plaintiffs' knowledge, Defendants have made no announcement or notification that they have remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

221. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

222. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

223. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the Data Breach to meet Defendants' contractual obligations and legal duties.

224. The hardship to Plaintiffs and Class Members if an injunction does not issue exceed the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs, Plaintiffs and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

225. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiffs and Class.

226. Plaintiffs and Class Members seek a declaration (i) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security; and (ii) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. engage internal security personnel to conduct testing, including audits on Defendants' systems, on a periodic basis, and promptly correct any problems or issues detected by such third-party security auditors;

b. engage third-party security auditors and internal personnel to run automated security monitoring;

c. audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for their provision of services;

e. conduct regular database scanning and security checks; and

f. routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, Private Information.

SIXTH CLAIM FOR RELIEF
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
Brought on Behalf of the Nationwide Class Against PSC and on Behalf of the Maximus Subclass Against Maximus

227. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 226 as if fully set forth herein.

228. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information that Defendants failed to safeguard and allowed to be accessed by way of the Data Breach.

229. Defendants' conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

230. By intentionally and/or knowingly failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

231. Defendants knew that an ordinary person in Plaintiffs' and Class Members' positions would consider Defendants' intentional actions highly offensive and objectionable.

232. Defendants invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' seclusion by intentionally failing to safeguard, misusing, and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

233. Defendants intentionally concealed from Plaintiffs and Class Members an incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

234. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information were unduly frustrated and thwarted.

235. Defendants' conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests, causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

236. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

237. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which

remains in Defendants' possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information

238. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

SEVENTH CLAIM FOR RELIEF
INVASION OF PRIVACY—PUBLIC DISCLOSURE OF PRIVATE FACTS
Brought on Behalf of the Nationwide Class Against PSC and on Behalf of the Maximus Subclass Against Maximus

239. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 238 as if fully set forth herein.

240. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendants mishandled.

241. As a result of Defendants' conduct, publicity was given to Plaintiffs' and Class Members' Private Information, which necessarily includes matters concerning their private life such as PII and PHI.

242. A reasonable person of ordinary sensibilities would consider the publication of Plaintiffs' and Class Members' Private Information to be highly offensive.

243. Plaintiffs' and Class Members' Private Information is not of legitimate public concern and should remain private.

244. As a direct and proximate result of Defendants' public disclosure of private facts, Plaintiffs and Class Members are at a current and ongoing risk of identity theft and sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft;

(d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) loss of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

245. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

246. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

EIGHTH CLAIM FOR RELIEF
BREACH OF CONFIDENCE
Brought on Behalf of the Nationwide Class Against PSC and on Behalf of the Maximus Subclass Against Maximus

247. Plaintiffs reallege and incorporate by reference preceding paragraphs 1 through 246 as if fully set forth herein.

248. Plaintiffs and Class Members have an interest, both equitable and legal, in Private Information conveyed to, collected by, and maintained by Defendants and ultimately accessed or compromised in the Data Breach.

249. Defendants have a special relationship with those whose Private Information they maintain, like Plaintiffs and the Class Members.

250. Because of that special relationship, Defendants were provided with and stored private and valuable Private information related to Plaintiffs and the Class, which they were required to maintain in confidence.

251. Plaintiffs and the Class provided Defendants with their Private Information under implied agreement of Defendants to limit the use and disclosure of such Private Information.

252. Defendants owed a duty to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in their possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

253. Defendants had an obligation to maintain the confidentiality of Plaintiffs' and the Class Members' Private Information. Plaintiffs and Class Members have a privacy interest in their personal medical matters, and Defendants had a duty not to disclose confidential Private Information.

254. As a result of the parties' relationship, Defendants had possession and knowledge of confidential Private Information of Plaintiffs and Class Members.

255. Plaintiffs' and the Class's Private Information is not generally known to the public and is confidential by nature.

256. Plaintiffs and Class Members did not consent to nor authorize Defendants to release or disclose their Private Information to an unknown criminal actor.

257. Defendants breached the duties of confidence they owed to Plaintiffs and Class Members when Plaintiffs' and the Class's Private Information was disclosed to unauthorized third parties.

258. Defendants breached their duties of confidence by failing to safeguard Plaintiffs' and Class Members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its own privacy policies and practices; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs and the Class Members' Private Information to a criminal third party.

259. But for Defendants' wrongful breach of their duty of confidences owed to Plaintiffs and Class Members, their privacy, confidences, and Private Information would not have been compromised.

260. As a direct and proximate result of Defendants' breach of Plaintiffs' and the Class's confidences, Plaintiffs and Class Members have suffered injuries, including: loss of their privacy and confidentiality in their Private Information; costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach; damages to and loss in value of

their Private Information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and mental anguish accompanying the loss of confidences and disclosure of their confidential and Private Information.

261. As a direct and proximate result of Defendants' breach of their duty of confidences, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

NINTH CLAIM FOR RELIEF
CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")
Cal. Civ. Code § 1798, *et seq*.
Brought on Behalf of California Subclass Against PSC and on Behalf of California Maximus Subclass Against Maximus

262. Plaintiff McCaskell realleges and incorporates by reference preceding paragraphs 1 through 261 as if fully set forth herein.

263. The California Legislature has explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[15]

264. The CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendants failed to implement such procedures which resulted in the Data Breach.

[15] California Consumer Privacy Act (CCPA) Compliance, https://buyergenomics.com/ccpa-complience/.

265. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

266. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

267. Plaintiff McCaskell and California class members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

268. Defendants are each a "business" as defined by Civ. Code § 1798.140(c) because each:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

269. The Private Information at issue is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiffs' and the California subclasses' members' unencrypted first and last names and Social Security numbers among other information.

270. Plaintiff and California subclass members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information, including name and contact information was wrongfully taken, accessed, and viewed by unauthorized third parties.

271. The Data Breach occurred as a result of Defendants' failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff McCaskell's and California subclass members' Private Information. Defendants failed to implement reasonable security procedures to prevent an attack on their server or network, including their email system, by hackers and to prevent unauthorized access of Plaintiff McCaskell's and California subclass members' Private Information as a result of this attack.

272. On June 11, 2024, Plaintiff McCaskell provided notice to Defendants pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiff alleges Defendants have violated or are violating. Although a cure is not possible under the circumstances, if (as expected) Defendants are unable to cure or do not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

273. Plaintiff McCaskell seeks all relief available under the CCPA including damages to be measured as the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

274. As a result of Defendants' failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff McCaskell seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

TENTH CLAIM FOR RELIEF
CALIFORNIA CONSUMER RECORDS ACT
Cal. Civ. Code § 1798.82, *et seq.*
Brought on Behalf of California Subclass Against PSC and on Behalf of California Maximus Subclass Against Maximus

275. Plaintiff McCaskell realleges and incorporates by reference preceding paragraphs 1 through 274 as if fully set forth herein.

276. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted

personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay. "

277. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code, § 1798.82(b).

278. Any person or business that is required to issue a security breach notification under the CCRA shall meet all of the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

    i. The name and contact information of the reporting person or business subject to this section;

    ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

    i. The date of the breach;

    ii. The estimated date of the breach; or

    iii. The date range within which the breach occurred. The notification shall also include the date of the notice.

d. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

e. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

f. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

279. The Data Breach described herein constituted a "breach of the security system" of Defendants.

280. As alleged above, Defendants unreasonably delayed informing Plaintiff McCaskell and California subclass members about the Data Breach, affecting their Private Information, after Defendants knew the Data Breach had occurred.

281. Defendants failed to disclose to Plaintiff McCaskell and the California subclass members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendants knew or reasonably believed such information had been compromised.

282. Defendants' ongoing business interests gave Defendants incentive to conceal the Data Breach from the public to ensure continued revenue.

283. Upon information and belief, no law enforcement agency instructed Defendants that timely notification to Plaintiff McCaskell and the California subclass members would impede its investigation.

284. As a result of Defendants' violation of California Civil Code section 1798.82, Plaintiff McCaskell and the California subclass members were deprived of prompt notice of the

Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff McCaskell and California subclass members because their stolen information would have had less value to identity thieves.

285. As a result of Defendants' violation of California Civil Code section 1798.82, Plaintiff McCaskell and the California subclass members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

286. Plaintiff McCaskell and the California subclass members seek all remedies available under California Civil Code section 1798.84, including, but not limited to the damages suffered by Plaintiff McCaskell and the other California subclass members, including but not limited to benefit-of-the-bargain and time spent monitoring their accounts for identity theft and medical identity theft, and equitable relief.

287. Defendants' misconduct as alleged herein is fraud under California Civil Code section 3294(c)(3) in that it was deceit or concealment of a material fact known to Defendants conducted with the intent on the part of Defendants of depriving Plaintiff McCaskell and the California subclass members of "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged herein is malice or oppression under California Civil Code section 3294(c)(1) and (c) in that it was despicable conduct carried on by Defendants with a willful and conscious disregard of the rights or safety of Plaintiff McCaskell and the California subclass members and despicable conduct that has subjected Plaintiff McCaskell and the California subclass members to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiff McCaskell and the California subclass members are entitled to punitive damages against Defendants under California Civil Code section 3294(a).

ELEVENTH CLAIM FOR RELIEF
CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT ("CMIA")
Cal. Civ. Code § 56, *et seq.*
Brought on Behalf of California Subclass Against PSC and on Behalf of California Maximus Subclass Against Maximus

288. Plaintiff McCaskell realleges and incorporates by reference preceding paragraphs 1 through 287 as if fully set forth herein.

289. Defendants are "contractor[s]" as defined in California Civil Code section 56.05(d), and are therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

290. As contractors, Defendants are required by the CMIA to ensure that medical information regarding patients is not disclosed or disseminated and/or released without patient's authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

291. Defendants are required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

292. Defendants are entities licensed under California's Business and Professions Code, Division 2.

293. Plaintiff and California class members are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("'Patient' means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains").

294. Furthermore, Plaintiff McCaskell and California subclass members, as patients and customers of Defendants, had their individually identifiable "medical information," within the

meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendants' computer network, and were patients on or before the date of the Data Breach.

295. Defendants disclosed "medical information," as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Defendants' employees, which allowed the hackers to see and obtain Plaintiff's and California class members' medical information.

296. Defendants negligently created, maintained, preserved, stored, and then exposed Plaintiff McCaskell's and California class members' individually identifiable "medical information," within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff's and California subclass members' names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities. Specifically, Defendants knowingly allowed and affirmatively acted in a manner that allowed unauthorized parties to access, exfiltrate, and actually view Plaintiff's and California subclass members' confidential Private Information.

297. Defendants' negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff McCaskell and California subclass members to unauthorized persons and the breach of the confidentiality of that information. Defendants negligently failed to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff McCaskell's and California subclass members' medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

298. Defendants also violated Sections 56.06 and 56.101 of the CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

299. Plaintiff McCaskell's and California subclass members' medical information was accessed and actually viewed by hackers in the Data Breach.

300. Plaintiff McCaskell's and California subclass members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

301. Defendants' computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A). As a direct and proximate result of Defendants' above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff McCaskell and the California subclass members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia:

a. present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud –risks justifying expenditures for protective and remedial services for which they are entitled to compensation;

b. invasion of privacy;

c. breach of the confidentiality of the Private Information;

d. statutory damages under the California CMIA;

g. loss of the value of their Private Information, for which there is well-established national and international markets; and/or,

h. the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

302. As a direct and proximate result of Defendants' wrongful actions, inactions, omissions, and want of ordinary care that directly and proximately caused the release of Plaintiff McCaskell's and California subclass members' Private Information, Plaintiff McCaskell's and California subclass members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiff McCaskell's and California subclass members' written authorization.

303. Defendants' negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff McCaskell's and California subclass members' medical information in a manner that preserved the confidentiality of the information contained therein violated the CMIA.

304. Plaintiff McCaskell and the California subclass members were injured and have suffered damages, as described above, from Defendants' illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorneys' fees, expenses, and costs.

TWELFTH CLAIM FOR RELIEF
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, *et seq.*
Brought on Behalf of California Subclass Against PSC and on Behalf of California Maximus Subclass Against Maximus

305. Plaintiff McCaskell realleges and incorporates by reference preceding paragraphs 1 through 304 as if fully set forth herein.

306. Defendants regularly do business in California. Defendants violated California's Unfair Competition Law ("UCL") (Cal. Bus. & Prof. Code, § 17200, et seq.) by engaging in unlawful, unfair, or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

a. by representing and advertising that they would maintain adequate data privacy and security practices and procedures to safeguard Private Information from unauthorized disclosure, release, data breach, and theft; representing and advertising that they did and would comply with the requirement of relevant federal and state laws pertaining to the privacy and security of the California class members' Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;

b. by soliciting and collecting California class members' Private Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's McCaskell and California subclass members' Private Information in an unsecure electronic environment;

c. by failing to disclose the Data Breach in a timely and accurate manner, in violation of California Civil Code section 1798.82;

d. by violating the privacy and security requirements of HIPAA, 42 U.S.C. §1302d, *et seq*.;

e. by violating the CMIA, California Civil Code section 56, et seq.; and

f. by violating the CCRA, California Civil Code section 1798.82.

307. These unfair acts and practices were immortal, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff McCaskell and California subclass members. Defendants' practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1302d, *et seq.*, CMIA, Cal. Civ. Code, § 56, *et seq.*, and the CCRA, Cal. Civ. Code, § 1798.81.5.

308. As a direct and proximate result of Defendants' unfair and unlawful practices and acts, Plaintiff McCaskell and the California subclass members were injured and lost money or property, including but not limited to the overpayments Defendants received to take reasonable and adequate security measures (but did not), the loss of their legally protected interest in the confidentiality and privacy of their Private Information, and additional losses described above.

309. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiff McCaskell's and California subclass members' Private Information and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff McCaskell and the California subclass members.

310. Plaintiff McCaskell seeks relief under the UCL, including restitution to the California subclass members of money or property that the Defendants may have acquired by means of Defendants' deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. Proc., § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as Class Representatives and undersigned counsel as Class Counsel;

B. Find in favor of Plaintiffs and the Class on all counts asserted herein;

C. Award Plaintiffs and the Class monetary damages, including actual and statutory, compensatory damages, general, consequential, nominal, and punitive damages, to the maximum extent as allowed by law;

D. Award restitution and all other forms of equitable monetary relief;

E. Award equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein regarding the misuse or disclosure of the private information of Plaintiffs and Class members, and from refusing to issue prompt, complete, and accurate disclosure to Plaintiffs and Class members;

F. Award injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, and to protect the interests of Plaintiffs and Class members, including but not limited to an order:

i. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

ii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class members unless Defendants can provide to the Court reasonable

justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class members;

iii. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class members;

iv. prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class members on a cloud-based database;

v. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

viii. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. requiring Defendants to conduct regular database scanning and securing checks;

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate;

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;

xvi. requiring, for a period of 10 years, the appointment of a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such

report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment;

xvii. requiring Defendants to implement multi-factor authentication requirements, if not already implemented; and

xviii. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices.

G. Award disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendants as a result of their unlawful acts;

H. Award a mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of their Private Information to unauthorized persons.

I. Order Defendants to purchase or provide funds for lifetime credit monitoring and identify theft insurance to Plaintiffs and Class Members;

J. Order Defendants to pay the costs of notifying Class Members about the judgment and administering the claims process.

K. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the maximum extent allowed by law;

L. Grant Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial;

M. Award Plaintiffs and the Class reasonable attorneys' fees, costs, and expenses, as allowable;

N. Distribute any monies recovered on behalf of Class Members or the general public via fluid recovery or cy pres recovery where necessary and as applicable to prevent Defendants from retaining benefits of their wrongful conduct;

O. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity; and

P. Award such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: June 17, 2024

Respectfully submitted,

/s/ Kristen A. Johnson
Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005

Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

Jeffrey S. Goldenberg
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

Plaintiffs' Vetting and Discovery Committee Member

Jason S. Rathod
Bruno Ortega-Toledo
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, D.C. 20002
Office: (202) 470-3520
jrathod@classlawdc.com
bortega@classlawdc.com

Mark DeSanto, Esq.
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
mdesanto@bm.net

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 17, 2024

/s/ Kristen Johnson
Kristen Johnson